



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/538,926	03/30/2000	Vance C. Bjorn	03022.P019	8632

7590 06/11/2007  
Judith A Szepesi  
Blakely Sokoloff Taylor & Zafman LLP  
7th floor  
12400 Wilshire Boulevard  
Los Angeles, CA 90025

EXAMINER
----------

MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
----------	--------------

2131

MAIL DATE	DELIVERY MODE
-----------	---------------

06/11/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



<b>Office Action Summary</b>	Application No. 09/538,926	Applicant(s) BJORN ET AL.	
	Examiner Aravind K. Moorthy	Art Unit 2131	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 23 March 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 March 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |



### DETAILED ACTION

1. This is in response to the arguments filed on 23 March 2007.
2. Claims 1-26 are pending in the application.
3. Claims 1-4, 7-9, 13, 14, 18, 19, 22 and 23 stand being rejected.
4. Claims 10-12 and 24-26 have been allowed.
5. Claims 5, 6, 15-17, 20 and 21 have been objected to.

### *Response to Arguments*

6. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claims 3-5, 10-12 and 24-26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

Claim 3 recites the limitation "the certificate" in the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim 4 recites the limitation "the user's private key" and "the user's temporary private key" in the claim. There is insufficient antecedent basis for this limitation in the claim.

Independent claim 10 recites "receiving a request for a certificate from the third party server" and "forwarding the request to a biometric certification server (BCS)". It is unclear to



Art Unit: 2131

the examiner as to which entity is receiving the request for a certificate. It is unclear to the examiner as to which entity is forwarding the request. Clarification is required.

Claim 24 recites the limitation "the user's private key" in the claim. There is insufficient antecedent basis for this limitation in the claim.

Independent claim 24 recites "a cryptographic engine to use the user's private key, as a virtual smart card". However, it is unclear to the examiner how the engine uses a private key as a virtual smart card. Clarification is required.

Any claims not directly addressed are rejected on the virtue of their dependency.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**8. Claims 1-3, 7-9, 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman et al U.S. Patent No. 6,012,039 in view of Ganesan U.S. Patent No. 5,535,276.**

As to claim 1, Hoffman et al discloses a client requesting a cryptographic service [column 9, lines 2-21]. Hoffman et al discloses establishing a secure connection between the client and a biometric certification server (BCS) [column 7, lines 21-21]. Hoffman et al discloses receiving biometric data from a user [column 9 line 44 to column 10 line 32]. Hoffman et al discloses that the BCS performs the cryptographic service if the user is authenticated based on the biometric data [column 9 line 44 to column 10 line 32].

Hoffman et al does not teach generating a disposable public key/private key pair.



Ganesan teaches generating a disposable public key/private key pair [column 8, lines 19-28].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al so that the public/private key pair would have been replaced by a disposable public key/private key pair.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al by the teaching of Ganesan, as described above, because it ensures that the key is not intercepted by a third party, by disposing of the key after its use [column 8, lines 19-28].

As to claim 2, Hoffman et al teaches that the cryptographic service is authenticating the user to another server [column 9 line 44 to column 10 line 32].

As to claim 3, Hoffman et al teaches certifying the public key. Hoffman et al teaches forwarding the certificate to the other server [column 10, lines 34-52].

As to claim 7, Hoffman et al teaches that the cryptographic service is signing or encrypting data [column 7, lines 12-21].

As to claim 8, Hoffman et al teaches that retrieving a private key/public key pair for the user. Hoffman et al teaches performing the cryptographic service with the private or the public key [column 7, lines 12-21].

As to claim 9, Hoffman et al teaches detecting an access to a certificate database of the client, as discussed above. Hoffman et al teaches detecting the user attempting to perform a cryptographic activity [column 7, lines 45-51].



As to claim 22, Hoffman et al discloses a crypto-API (application program interface) for receiving cryptographic function requests [column 9, lines 2-21]. Hoffman et al discloses a cryptographic service provider for establishing a secure connection to a remote crypto-server [column 7, lines 21-21]. Hoffman et al discloses having the crypto-server perform the cryptographic function [column 9 line 44 to column 10 line 32]. Hoffman et al discloses a sensor for receiving biometric data from a user [column 9 line 44 to column 10 line 32]. Hoffman et al discloses that the biometric data is sent to the crypto-server to authenticate the user and that the remote crypto-server is to perform the requested cryptographic function when the user is successfully authenticated using the biometric data [column 9 line 44 to column 10 line 32].

Hoffman et al does not teach generating a disposable public key/private key pair.

Ganesan teaches generating a disposable public key/private key pair [column 8, lines 19-28].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al so that the public/private key pair would have been replaced by a disposable public key/private key pair.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al by the teaching of Ganesan, as described above, because it ensures that the key is not intercepted by a third party, by disposing of the key after its use [column 8, lines 19-28].

As to claim 23, Hoffman et al discloses a crypto-API (application program interface) for receiving cryptographic function requests [column 9, lines 2-21]. Hoffman et al discloses a cryptographic service provider for establishing a secure connection to a remote crypto-server.



Hoffman et al discloses having the crypto-server perform the cryptographic function [column 9 line 44 to column 10 line 32]. Hoffman et al discloses a sensor for receiving biometric data from a user, as discussed above. Hoffman et al discloses that the biometric data sent to the crypto-server to authenticate the user [column 9 line 44 to column 10 line 32]. Hoffman et al discloses that the remote crypto-server comprises: a crypto-proxy interface for receiving a request for the cryptographic function from the client on the secure connection; an authentication engine for authenticating the user based on the biometric data; a cryptographic engine for performing the cryptographic functions; and the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed [column 9 line 44 to column 10 line 32].

Hoffman et al does not teach generating a disposable public key/private key pair.

Ganesan teaches generating a disposable public key/private key pair [column 8, lines 19-28].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al so that the public/private key pair would have been replaced by a disposable public key/private key pair.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al by the teaching of Ganesan, as described above, because it ensures that the key is not intercepted by a third party, by disposing of the key after its use [column 8, lines 19-28].



**9. Claims 13-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman et al U.S. Patent No. 6,012,039 in view of Jakobsson U.S. Patent No. 6,587,946 B1.**

As to claim 13, Hoffman et al discloses an authentication engine for authenticating the user based on biometric data [column 9 line 44 to column 10 line 32]. Hoffman et al discloses a cryptographic engine for performing the cryptographic functions, as discussed above.

Hoffman et al does not teach a crypto-server having a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection. Hoffman et al does not teach that the crypto-proxy interface returns data to the client, after the cryptographic functions are performed.

Jakobsson teaches a crypto-server having a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection [column 5, lines 48-64]. Jakobsson teaches that the crypto-proxy interface returns data to the client, after the cryptographic functions are performed [column 6, lines 3-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al so that the authentication engine would have authenticated the user based on biometric data received through a crypto-proxy interface of the crypto-server. A crypto-server would have had a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection. A cryptographic engine would have performed the cryptographic functions after the authentication engine authenticated the user based on the biometric data. The crypto-proxy interface would have returned the data to the client, after the cryptographic functions was performed.



It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al by the teaching of Jakobsson because it is efficient, allows tight control over actions (by the use of quorum cryptography), does not require any pre-computation phase to set up shared keys, and has a trust model appropriate for a variety of settings [column 3, lines 50-58].

As to claim 14, Hoffman et al teaches that a database includes user credentials [0034]. Hoffman et al teaches that the authentication engine retrieving user biometric template from the database and comparing the biometric template to the biometric data received from the user [column 9 line 44 to column 10 line 32].

As to claim 18, Hoffman et al suggests a user self-registration interface permitting a user to choose a handle and register a biometric template [column 9 line 44 to column 10 line 32].

As to claim 19, Hoffman et al teaches a registration engine for receiving biometric data from the user during a registration process [column 6, lines 40-65]. Hoffman et al teaches extracting the biometric template for the user [column 6, lines 40-65]. Hoffman et al teaches a user credential database for storing the handle and the biometric template of the user [column 6, lines 40-65].



*Allowable Subject Matter*

**10. Claims 10-12 and 24-26 are allowed.**

As to independent claim 10, Prior art does not disclose, teach or fairly suggest receiving a request for a certificate from the third party server. Prior art does not disclose, teach or fairly suggest forwarding the request to a biometric certification server (BCS). Prior art does not disclose, teach or fairly suggest receiving a biometric identification from the client and forwarding the biometric identification to the BCS. Prior art does not disclose, teach or fairly suggest that if the biometric identification matches a registered user on the BCS, receiving a certificate including a public key of the client certified by the BCS. Prior art does not disclose, teach or fairly suggest forwarding the certificate, including the public key of the client certified by the BCS, to the third party server, thereby identifying the client to the third party server.

As to independent claim 24, Prior art does not disclose, teach or fairly suggest a cryptographic engine to use a user's private key, as a virtual smart card, to perform a requested cryptographic function after the user has been authenticated by the authentication engine.

Any claims not directly addressed are allowed on the virtue of their dependency.

11. Claims 4-6, 15-17, 20 and 21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.




*Conclusion*

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy   
June 2, 2007

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100